

MS#180490.1 (4969)
PATENT

REMARKS

Applicant has thoroughly considered the Examiner's remarks. The application has been amended to more clearly set forth the invention. Claims 1-46 are presented in the application for further examination. Claims 1, 15-20, 22-26, 29, 38, 40, 42 and 44 have been amended by this Amendment A. Reconsideration of the application claims as amended and in view of the following remarks is respectfully requested.

RESPONSE TO REJECTION BASED ON 35 USC 102(e)

As specified in paragraphs 6-23 of the Office action, Claims 22, 24, 26, 28, 40 and 41 stand rejected as unpatentable over Desai, claim 23 stand rejected as unpatentable over Desai in view of Robertson and claims 25 and 27 stand rejected as being unpatentable over Desai in view of Kramer. Claims 22 and 40 are independent. Applicant submits that amended independent claims 22 and 40 are patentable over Desai, Robertson and Kramer, either taken separately or in combination, so that the rejection based on 35 USC 102(e) should be withdrawn.

Claim 22 has been amended to more clearly recite a user-centric method that relates to permitting certain clients (separate and apart from a user) the selective right to access user-specific information according user controlled access. In particular, claim 25 has been amended to recite:

A user-centric method of controlling access to user specific information in a network computing environment, said network computing environment including a web-services provider and a user of a service provided by the web-services provider, the web-services provider maintaining a data store of use-specific information associated with the user, **said user-specific information accessible by the user and having access by the clients controlled by the user,** the user communicating with the web-services provider via a network communication device having a display interface and a selection interface, said user-centric method of controlling access to user-specific information comprising:

identifying the user;

identifying a plurality of clients of the web-services provider wherein the user desires to grant access to the user-specific information in the data store to **certain of the plurality of clients;**

identifying a method of access by which the user is willing to allow the **certain clients** to access the user-specific information in the data store;

identifying a level of access to the user-specific information in the data store the user desires to impose on the **certain clients;** and

MS#180490.1 (4969)
PATENT

writing an access control rule to an access control list associated with said data store, said access control rule limiting access to the user-specific information in the data store by the certain clients to the identified method of access and the identified level of access.

Similarly, claim 40 has been amended to more clearly recite a user-centric method that relates to permitting a third party (separate and apart from a user) the selective right to access certain user-specific information according user controlled access. In particular, claim 40 has been amended to recite:

A method of controlling access to user specific information by a third party in a network computing environment, said network computing environment including a web-services provider, a user of a service provided by the web-services provider, the web-services provider maintaining a data store of user-specific information associated with the user, said user-specific information accessible by the user and having access by the third party controlled by the user, the third party in digital communication with the web-services provider, the third party desiring access to certain of the user-specific information in the data store, and the user communicating with the web-services provider via a network communication device having a display interface and a selection interface, said method of controlling access to user-specific information by the third party comprising:

obtaining at the web-services provider a digital request message from the third party desiring access to the certain user-specific information in the data store;

determining an intended purpose of the third party for accessing the certain user-specific information in the data store;

generating an option list having at least one entry therein based on the determined intended purpose of the third party for accessing the certain user-specific information in the data store;

displaying to the user on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option using the selection interface of the network communication device;

receiving from the network communication device a selection signal indicative of whether the user accepted or rejected the at least one option; and

creating an access control rule based on the received selection signal, said access control rule defining an extent of access to the certain user-specific information in the data store granted to the third party.

The primary references cited and applied by the Examiner to reject claims 22 and 40 is Desai relating to selective information exchange. However, Desai contemplates that the user grants access on an element-by-element basis and on a

MS#180490.1 (4969)
PATENT

person-by-person basis:

The registered user may selectively grant access to each view to one or more third parties, such as friends or family members. (column 4, lines 2-4).

The registered user may create a view of one or more data elements, and access to one or more views may be granted to one or more groups of users created by the registered user. In the preferred embodiment, pre-defined views and groups are also provided.

After access has been granted, it can be denied on an element-by-element and person-by-person basis. (column 5, lines 51-58).

The information exchange system 10 further includes facilities that allow the registered user 12 to selectively grant access to this stored profile data to one or more third parties 17a-c on an element-by-element basis. As illustrated in tables 18 and 20, the registered user 12 granted an online vendor 17a access to its telephone number, street address and credit card number, and a business contact 17b was granted access to the registered user's telephone number. (column 9, lines 10-18).

Thus, Desai fails to recognize an "access control rule" as recited by claims 22 and 40 which grants selected access to clients/third parties, not according to an element-by-element basis and a person-by-person basis. For example, according to one embodiment of the invention, a client may be permitted to access certain user information even though the client has not previously specifically been authorized access by the user.

The Examiner cites column 9, lines 19-22 and column 13, lines 25-33 to support the rejection. These sections of Desai relate to a vendor retrieving purchase information and matching a merchant's public key to the user's secret key. There is no mention of an access control rule in the context of an identified method of access and an identified level of access as recited by claim 22. Also, there is no mention of an access control rule in the context of the determined intended purpose of the third party and an option list based thereon to access certain user-specific information, as recited by claim 40.

The remaining references, as will be pointed out below, are similarly deficient. Thus, the 102(e) rejection of independent claims 22 and 40, and claims 24, 26, 28, and 41 depending therefrom, should be withdrawn.

MS#180490.1 (4969)
PATENT

RESPONSE TO REJECTION BASED ON 35 USC 103(a)

As specified in paragraphs 24-37 of the Office action, claims 15-19 and 21 stand rejected as unpatentable over Orita in view of Desai and claim 20 stands rejected as being unpatentable over Orita in view of Desai and Kramer. Claim 15 is independent. Applicant submits that amended independent claim 15 is patentable over Orita, Desai and Kramer, either taken separately or in combination, so that the rejection based on 35 USC 103(a) should be withdrawn.

Claim 15 has been amended to more clearly recite a method controlling client access to certain user-specific information according user controlled access based on an intended use by the client and an allowed level of access permitted by the user. In particular, claim 15 has been amended to recite:

A method of controlling access to user specific information for use in a network computer system including a web-services provider, a user of a service provided by the web-services provider, and a client of the web-services provider, said web-services provider maintaining a data store of user-specific information associated with the user, **said user-specific information accessible by the user and having access by the client controlled by the user**, said client seeking access to **certain** of the user-specific information in the data store, said method of controlling access to the user-specific information comprising:

operatively receiving at the web-services provider a request from the client to access the certain user-specific information in the data store;

determining *an intended use* by the client of the **certain user-specific information in the data store**;

determining *an allowed level of access* permitted by the user;

comparing the determined intended use with the determined allowed level of access; and

completing the request from the client to access the **certain user-specific information in the data store** when the **determined intended use** by said client of the certain user-specific information is within the **determined allowed level of access** permitted by the user.

The primary references cited and applied by the Examiner to reject claim 15 is Orita describing a computer system with file security functions. However, Orita contemplates that only registered users have access to all of their profiles. Applicant fails to see any teaching in Orita which would permit a client, separate from the user, to have selected access. Orita fails to recognize controlling client access to certain user-

MS#180490.1 (4969)
PATENT

specific information according user controlled access based on an intended use by the client and an allowed level of access permitted by the user, as recited by claim 15.

The Examiner cites various lines of column 4 of Orita to support the rejection. These sections of Orita relates to controlling access based on passwords and access protection information. There is no mention of determining an intended client use, determining an allowed level of access and providing access to certain user-specific information based thereon, as recited by claim 15.

Desai is deficient with regard to claim 15 for the same reasons as noted above in the context of claims 22 and 40.

Applicant submits the Kramer is also deficient for the same reasons. In addition, the Examiner cites Kramer as teaching updating the access control list and refers to column 4, lines 1-5 and 52-55. However, these sections of Kramer relate to access with respect to an authorized user, not in the context of a client accessing selected user-specific information as recited by claim 15.

The remaining references, as pointed out herein, are similarly deficient. Thus, the 103(a) rejection of independent claim 15, and claims 16-19 and 21 depending therefrom, should be withdrawn.

As specified in paragraphs 38-82 of the Office action, claims 1-3, 7, 8, 10, 14, 29, 30, 35, 36, 38, 39, and 44-46 stand rejected as unpatentable over Orita in view of Bradee and Desai. Claims 4, 5, 13, 31-34 and 37 stand rejected as being unpatentable over Orita in view of Bradee, Desai and Kramer. Claim 6 stands rejected as being unpatentable over Orita in view of Bradee, Desai and Allgeier. Claim 9 stands rejected as being unpatentable over Orita in view of Bradee, Desai and Robertson. Claims 11 and 12 stand rejected as being unpatentable over Orita in view of Bradee, Desai and Erickson. Claims 1, 29, 38 and 44 are independent. Applicant submits that amended independent claims 1, 29, 38 and 44 are patentable over Orita, Bradee, Desai, Kramer, Allgeier, Robertson and Erickson, either taken separately or in combination, so that the rejection based on 35 USC 103(a) should be withdrawn.

Claims 1, 29, 38 and 44 have been amended to more clearly recite a method controlling client access to user-specific information according user controlled access based on an intended use by the client and an allowed level of access permitted by the

MS#180490.1 (4969)
PATENT

user. For example, claim 1 is representative and has been amended to recite:

A method of controlling access to user-specific information for use in connection with a network computing environment including a web-services provider providing a web-based software service, said method of controlling access to the user-specific information comprising:

providing a user access to a service provided by the web-services provider, said web-services provider maintaining a data store of user-specific information associated with the user in connection with the service, said web-services provider maintaining an access control list identifying when the user grants a form of access to a client wherein the form of access granted to the client is limited to certain user-specific information;

providing a client access to the service provided by the web-services provider, said client seeking access to some of the user-specific information maintained in the data store;

obtaining an access request message from the client and directed to the software service requesting user-specific information, said request message including an access request parameter indicating the client's requested form of access to the user-specific information in the data store;

comparing the access request parameter to an access control list associated with the software service; said access control list identifying whether the user has granted the form of access requested by the client;

permitting the client to have access to the requested user-specific information in the data store if the user has granted the form of access requested by the client; and

invoking an access control engine if the user has not previously granted the form of access requested by the client, said access control engine:

determining an intended use by the client of the requested user-specific information in the data store;

comparing the determined intended use by the client with a default access control instruction;

updating the access control list to permit the client to have access to the requested user-specific information in the data store if the default access control instruction permits the determined intended use; and

transmitting a fault response to the client if the default access control instruction does not permit the determined intended use.

The primary references cited and applied by the Examiner to reject claim 15 is Orita describing a computer system with file security functions. However, as noted above, Orita contemplates that only registered users have access to all of their profiles. More importantly, Orita does not suggest an access control engine permitting certain intended uses by a third-party client in combination with dynamic updating. Applicant

MS#180490.1 (4969)
PATENT

fails to see any teaching in Orita which would permit a client, separate from the user, to have selected access in the context of dynamic updating.

The Examiner cites various lines of column 4, line 65 to column 5, line 1, of Orita to support the rejection. The Examiner argues that these sections of Orita relate to a "host computer determines if client is provided the form of access by either allowing or denying access." However, this part of Orita relates to data managers in a hierarchy. There is no mention of an access control engine which is invoked when the user has not previously granted the form of access requested by the client. Further, the access control engine determines an intended use by the client, comparing the determined intended use by the client with a default access control instruction, and dynamically updates the access control list, as recited by claim 1. This combination is not found in Orita.

The Examiner admits that Orita does not teach dynamic updating and cites Bradlee. Yet, Bradlee is also deficient because paragraph 62 of page 8 of Bradlee teaches "dynamically updating conditions to determine whether a user should be permitted access to a resource" not a client permitted access to user-specific information, as recited by claim 1.

Desai is deficient with regard to claim 1 for the same reasons as noted above in the context of claims 15, 22 and 40.

Applicant submits the Kramer is also deficient for the same reasons. In addition, the Examiner cites Kramer as teaching updating the access control list and refers to column 4, lines 1-5 and 52-55. However, these sections of Kramer relate to access with respect to an authorized user, not in the context of a client accessing selected user-specific information as recited by claim 1.

The Examiner cites Allegeier as teaching "an invention where a determination is made if a selected data is stored in a first database." This relates to databases and fails to recognize any applicability with respect to has client/user access. The Examiner cites Robertson as teaching "an invention for managing which clients may have access to user information." However, access is based on granted permissions, not an access control engine. The Examiner cites Erickson as teaching "an invention for transmitting messages according to the SOAP protocol." However,

MS#180490.1 (4969)
PATENT

Erickson relates to message exchange, not which clients may have access to user information.

Applicant requests that the Examiner specify the teaching for combining the Bradee, Allgeier, Robertson and Erickson references with Orita or Desai. Without such a teaching, the obviousness rejection falls short and must be withdrawn. "[T]he question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination." Lindemann MaschinenFabrick GMBH v. American Hoist and Derrick Company, 730 F.2d 1452, 1462; 221 U.S.P.Q. 481, 488 (Fed. Cir. 1984). As has been shown above, the incomplete teachings of the prior art are directed to entirely different problems. Therefore, nothing in the cited references suggests their combination. Indeed, the Examiner failed to cite any basis whatsoever for combining these references.

In fact, the Examiner's rejection provides a textbook example of impermissible hindsight analysis -- the Examiner used the invention as defined by the claims as a guide to pick and choose unrelated references in order to reject the claims. See In re Oetiker, 977 F.2d at 1447; 24 U.S.P.Q.2d at 1446 (Fed. Cir. 1992) ("There must be some reason, suggestion, or motivation found in the prior art whereby a person of ordinary skill in the field of the invention would make the combination. That knowledge can not come from the applicant's invention itself.").

The remaining references, as pointed out herein, are similarly deficient. Thus, the 103(a) rejection of independent claims 1, 29, 38 and 44, and claims 2-3, 7, 8, 10, 14, 30, 35, 36, 39, 45-46, 4, 5, 13, 31-34, 37, 6, 9, 11 and 12 depending therefrom, should be withdrawn.

As specified in paragraph 83-91 of the Office action, claims 42 and 43 stand rejected as unpatentable over Orita in view of Bradee and Kramer. Claim 42 is independent. Applicant submits that amended independent claim 42 and its dependent claim 43 are patentable over Orita, Bradee, and Kramer, either taken separately or in combination, for the same reasons as noted above with regard to the other independent claims so that the rejection based on 35 USC 103(a) should be withdrawn. For example, claim 42 recites certain user-specific information related to an intentions document. Such is not in the combined references.

MS#180490.1 (4969)
PATENT

CONCLUSION

It is felt that a full and complete response has been made to the Office action and, as such, places the application in condition for allowance. Such allowance is hereby respectfully requested.

Applicant wishes to expedite prosecution of this application. If the Examiner deems the claims as amended to not be in condition for allowance, the Examiner is invited and encouraged to telephone the undersigned to discuss making an Examiner's amendment to place the claims in condition for allowance.

Applicant does not believe that a fee is due in connection with this response. If, however, the Commissioner determines that a fee is due, he is authorized to charge Deposit Account No. 19-1345.

Respectfully submitted,



Frank R. Agovino, Reg. No. 27,416
SENNIGER POWERS
One Metropolitan Square, 16th Floor
St. Louis, Missouri 63102
(314) 231-5400

FRA/cwa